NATIONAL COMPUTER SECURITY CENTER

Introduction
to
Certification
and
Accreditation

January 1994

FOREWORD

The National Computer Security Center is publishing *Introduction to Certification and Accreditation* as part of the "Rainbow Series" of documents our Technical Guidelines Program produces. This document initiates a subseries on certification and accreditation (C&A) guidance, and provides an introduction to C&A including an introductory discussion of some basic concepts related to C&A, and sets the baseline for future documents on the same subject. It is not intended as a comprehensive tutorial or manual on the broad topic of information systems security. It should be viewed, instead, as guidance in meeting requirements for certification and accreditation of automated information systems.

The combination of the information age, technology, and national policy, has irrevocably pushed us into an Information Systems Security age. The explosion in the uses of telecommunication devices and automated information systems has resulted in a corresponding explosion in opportunities for unauthorized exploitation of valuable information. The technology necessary to perform this exploitation is available not only to our foreign adversaries but also to criminal elements.

As the Director of the National Computer Security Center, I invite your suggestions for revising this document. We plan to review and revise this document as the need arises. Please address all proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

Attention: Chief, Standards, Criteria, and Guidelines Division

January 1994

Patrick R. Gallagher, Jr.
Director
National Computer Security Center

ACKNOWLEDGMENTS

ABSTRACT

This document, which provides an introduction to certification and accreditation (C&A) concepts, provides an introductory discussion of some basic concepts related to C&A and sets the baseline for further documents. Its objectives are the following: (1) to provide an overview of C&A, its function and place within the risk management process; (2) to clarify the critical roles the Designated Approving Authority (DAA) and other key security officials must assume throughout the C&A process; (3) to identify some of the current security policies, emphasizing some key policy issue areas; and (4) to define C&A-related terms. The details of the actual C&A process are not included in this document, but will be provided in a follow-on document(s).

Suggested Keywords: certification, accreditation, Designated Approving Authority (DAA), INFOSEC, security policy

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

1.1 Background

In recent years, there has been a shift in perspective of information systems security (INFOSEC) from viewing it as a number of independent, loosely coupled disciplines to a more cohesive, interdependent collection of security solutions. The current environment of declining resources and the rapid advances in technology have demanded changes in assessing the security posture of systems and implementing an INFOSEC systems engineering process. These changes are necessary to reduce fragmentation and to ensure and maintain consistency and compatibility among all aspects of the security of a system. In addition, the dynamic threat environment necessitates a more efficient, integrated view of INFOSEC disciplines.

In considering the overall security of a system, two essential concepts are (1) that the (security) goals of the system be clearly stated and (2) that an analysis be made of the ability of the system to (a) satisfy the original goals and (b) continue to provide the attributes and security required in the evolving environment. The Department of Defense (DoD) and other federal agencies have formalized these concepts. DoD policy states that any automated information system (AIS) that processes classified, sensitive unclassified, or unclassified information must undergo a technical analysis and management approval before it is allowed to operate [1]. The technical analysis establishes the extent to which the system meets a set of specified security requirements for its mission and operational environment. The management approval is the formal acceptance of responsibility for operating at a given level of risk. The technical analysis and management approval processes are called certification and accreditation (C&A), respectively. These concepts, however, are quite general and can be applied with different levels of formality and within different organizational structures.

One of the most important tasks required to provide an integrated, cost-effective information systems security program, is to develop uniform certification and accreditation guidance. The use of AISs within all aspects of operations, the dynamic organization of systems, and the exchange of information among systems point to the need for uniform guidance when certifying and accrediting systems. The National Security Agency (NSA), in support of its mission to provide guidelines on the acquisition, certification, accreditation, and operation of systems, plans to publish a series of documents focusing on these issues. This introductory document discusses

1

the basic concept of C&A of systems in an effort to provide improvements in the secure development, operation, and maintenance of systems.

1.2   Scope

This document provides an overview to some basic concepts and policies of C&A. Individuals serving as system accreditors, system certifiers, program managers (PMs), developers, system integrators, system engineers, security officers, evaluators, and system users will benefit from this document by gaining a basic understanding of C&A. People in each of the many roles involved in C&A will have a different focus and emphasis on related activities. Therefore, it is important that everyone involved has a basic understanding of the high-level process and uses common terminology. This document provides a basic overview of C&A, but it is not a replacement for reviewing and understanding the specific national, federal, department, and service/agency policies and guidelines in the actual performance of C&A.

The concepts of C&A presented in this document apply to all types of systems: existing and proposed systems, stand-alone systems, personal computers (PCs), microcomputers, minicomputers, mainframes, large central processing facilities, networks, distributed systems, embedded systems, workstations, telecommunications systems, systems composed of both evaluated and unevaluated components, other security components, and systems composed of previously accredited systems (particularly when some of these accredited systems have not been certified or have been certified against differing criteria). Guidance on applying the high-level C&A process to particular types of systems, as well as associated activities, will be provided in subsequent documents in this series.

1.3   Purpose

The purpose of this C&A concepts document is to discuss the high-level C&A process, authority for C&A, C&A policy, and C&A terminology. This document sets the baseline for a series of documents and has the following objectives:

- Discuss the high-level C&A process and its relationship to risk management and INFOSEC disciplines.

- Clarify the critical roles the DAA and key security officials must assume throughout the C&A process.

- Identify several current security policies, emphasizing areas that are ambiguous or not addressed in current policy.

- Define basic C&A terms.

2

1.4 Evaluation Versus Certification

Evaluation is a term used in many different ways causing much confusion in the security community. Sometimes it is used in the general English sense meaning judgment or determination of worth or quality. Based on common usage of the term in the security community, one can distinguish between two types of evaluations: (1) evaluations that exclude the environment, and (2) evaluations that include the environment. This second type of evaluation, meaning an evaluation conducted to assess a systems security attributes with respect to a specific operational requirement(s), is what this series of documents refers to as certification. Evaluations that exclude the environment are analysis against a standard or criteria. There are a number of examples of this type of evaluation:

- Commercial off-the-shelf (COTS) products evaluated against the Trusted Computer System Evaluation Criteria (TCSEC) (Orange Book) [2] or the Canadian or European Criteria

- Compartmented Mode Workstations (CMW) evaluated against the *Compartmented Mode Workstation Evaluation Criteria, Version 1* (CMWEC) [3] and the TCSEC

- Communications products with embedded communications security (COMSEC) components evaluated against the FSRS (*NSA Specification for General Functional Security Requirements for a Telecommunications System (FSRS)* [4])

- Products evaluated against the TEMPEST criteria (DoD Directive (DoDD) C-5200.19 [5])

Products that have been evaluated against the FSRS and that satisfactorily meet the minimum requirements (and are successfully considered for NSA approval) are generally said to be endorsed products. Products evaluated against the TCSEC are often referred to as evaluated products. While current usage of these terms varies widely, in this document, the term evaluation will refer to a security analysis of a component against a given set of standards or criteria without regard to the environment, while certification refers to a security analysis of a system against a given set of security requirements in a given environment.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 2

OVERVIEW OF C&A

Certification and accreditation constitute a set of procedures and judgments leading to a determination of the suitability of the system in question to operate in the targeted operational environment.

Accreditation is the official management authorization to operate a system. The accreditation normally grants approval for the system to operate (a) in a particular security mode, (b) with a prescribed set of countermeasures (administrative, physical, personnel, COMSEC, emissions, and computer security (COMPUSEC) controls), (c) against a defined threat and with stated vulnerabilities and countermeasures, (d) within a given operational concept and environment, (e) with stated interconnections to other systems, (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (g) for a specified period of time. The Designated Approving Authority(s) (DAA) formally accepts security responsibility for the operation of the system and officially declares that the specified system will adequately protect against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the DAA and shows that due care has been taken for security in accordance with the applicable policies.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the DAA, and remains in effect for the specified period of time (varies according to applicable policies). A system processing classified or sensitive unclassified information should be accredited prior to operation or testing with live data unless a written waiver is granted by the DAA. In some cases (e.g., when dealing with new technology, during a transition phase, or when additional time is needed for more rigorous testing), the DAA may grant an interim approval to operate for a specified period of time. At the end of the specified time period, the DAA must make the final accreditation decision.

Certification is conducted in support of the accreditation process. It is the comprehensive analysis of both the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets the security requirements for its mission and operational environment. A complete system certification must consider factors dealing with the system in its unique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, system configuration, site/facility location, and interconnections with other systems. Certification should be done by personnel who are technically competent to assess the systems ability to meet the security

5

requirements according to an acceptable methodology. The resulting documentation of the certification activities is provided to the DAA to support the accreditation decision. Many security activities support certification, such as risk analysis, security test and evaluation, and various types of evaluations.

Ideally, certification and accreditation procedures encompass the entire life cycle of the system. Ideally, the DAA is involved from the inception of the system to ensure that the accreditation goals are clearly defined. A successful certification effort implies that system security attributes were measured and tested against the threats of the intended operational scenarios. Additionally, certification and accreditation are seen as continuing and dynamic processes; the security state of the system needs to be tracked and assessed through changes to the system and its operational environment. Likewise, the management decision to accept the changing system for continued operation is an ongoing decision process. The following sections provide a description of risk management, the high-level C&A process, and recertification/reaccreditation.

2.1 Risk Management and C&A

Risk management is the total process of identifying, measuring, and minimizing uncertain events affecting resources [1]. A fundamental aspect of risk management is the identification of the security posture (i.e., threats and vulnerabilities) of the system, and stating the characteristics of the operational environment from a security perspective. The primary objective of risk management is to identify specific areas where safeguards are needed against deliberate or inadvertent unauthorized disclosure, modification of information, denial of service, and unauthorized use. Countermeasures can then be applied in those areas to eliminate or adequately reduce the identified risk. The results of this activity provide critical information to making an accreditation decision.

Risk management may include risk analysis, cost-benefit analysis, countermeasure selection, security test and evaluation (ST&E), countermeasure implementation, penetration testing, and systems review. For DoD organizations, enclosure 3 to DoDD 5200.28 mandates a risk management program for each AIS to determine how much protection is required, how much exists, and the most economical way of providing the needed protection. Other federal departments and agencies have similar policy documents that should be referenced for guidance

Risk analysis minimizes risk by specifying security measures commensurate with the relative values of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them. Risk analysis should be applied iteratively during the system life cycle. When applied to system design, a risk analysis aids in countermeasure specification. When applied during the implementation phase or to an operational system, it can verify the effectiveness of existing countermeasures and identify areas in which additional measures are needed to achieve the desired level of security. There are numerous risk analysis methodologies and some automated tools available to support them.

Management commitment to a comprehensive risk management program must be defined as early as possible in the program life cycle. In scheduling risk management activities and designating resources, careful consideration should be given to C&A goals and milestones. Associated risks can then be assessed and corrective action considered for risks that are unacceptable.

2.2 C&A High-Level Process

The C&A process is a method for ensuring that an appropriate combination of security measures are implemented to counter relevant threats and vulnerabilities. This high-level process consists of several iterative, interdependent phases and steps illustrated in Figure 2.1. The scope and specific activities of each step depend upon the system being certified and accredited (see section 2.2.2).

Step 1 of the C&A process focuses on identifying and assessing the specific security-relevant aspects (i.e., tailoring factors) of a system. It involves gathering and developing relevant documentation (e.g., policy implementation guidance, security regulations/manuals, previous certification reports, product evaluation reports, COTS manuals, design documentation, design modification, and security-related waivers). This identification provides the foundation for subsequent phases, and is critical to determining the appropriate C&A tailoring guidance to be used throughout the C&A process. Aspects to be considered include:

- Mission criticality
- Functional requirements
- System security boundary
- Security policies
- Security concept of operations (CONOPS)
- System components and their characteristics
- External interfaces and connection requirements
- Security mode of operation or overall risk index
- System and data ownership
- Threat information
- Identification of the DAA(s)

Step 2 involves C&A planning. Since security should have been considered with system conception, planning for C&A is a natural extension of system security planning. That is, the schedule (milestones) and resources (e.g., personnel, equipment, and training) required to complete the C&A process are identified. C&A planning information is incorporated into and maintained in program documentation. This information is also used to estimate the C&A budget. Aspects to be considered in this step include:

- Reusability of previous evidence
- Life-cycle phase
- System milestones (time constraints)

7
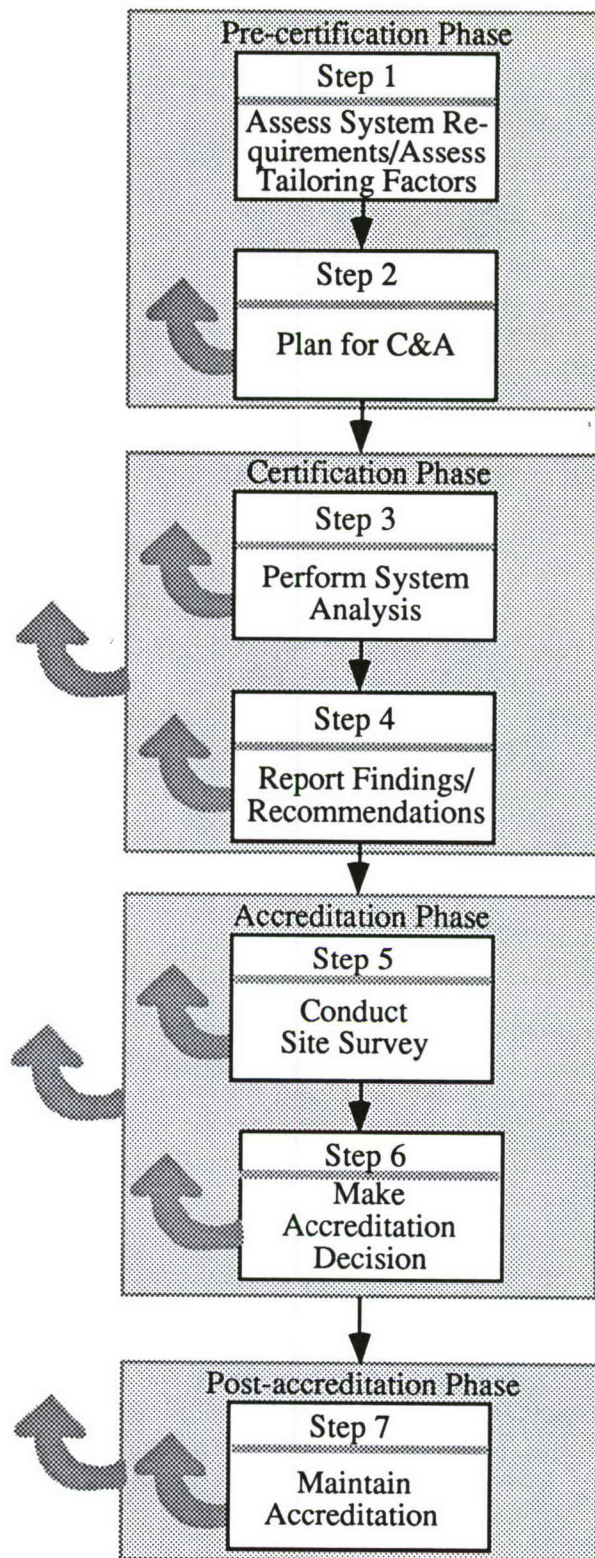
Figure 2.1. High-Level C&A Process

Step 3 involves analyzing the security aspects of the system as a whole (i.e., how well security is employed throughout the system). During this phase, the certification team becomes more familiar with the security requirements and the security aspects of individual system components. Specialized training on the specific system may be necessary depending upon the scope of this phase as well as the experience of the certification team. C&A activities include determining whether system security measures adequately satisfy applicable requirements. To accomplish this objective, security measures of the various disciplines are assessed and tested collectively. Additionally, system vulnerabilities and residual risks are identified.

Step 4 involves documenting/coordinating the results and recommendations of previous phases to prepare the certification package and accreditation package. The certification package is the consolidation of all the certification activity results. It will be used as supporting documentation for the accreditation decision, and will also support recertification/reaccreditation activities. The compilation of the supporting documentation should be done consistently and cost-effectively. The types of documentation generally included as part of the certification package include:

- System need/mission overview

- Security policy

- Security concept of operation or security plan

- System architectural description and configuration

- Reports of evaluated products from a recognized government evaluation (e.g., NSA product evaluation, the Defense Intelligence Agency (DIA)/NSA compartmented mode workstation (CMW) evaluation)

- Statements from other responsible agencies indicating that personnel, physical, COMSEC, or other security requirements have been met (e.g., Defense Message System (DMS) component approval process (CAP) functional testing)

- Risks and INFOSEC countermeasures (e.g., risk analysis report)

- Test plans, test procedures, and test results from security tests conducted (including penetration testing)

- Analytic results

- Configuration Management plan

- Previous C&A information

- Contingency plan

9

The accreditation package presents the DAA with a recommendation for an accreditation decision, a statement of residual risk, and supporting documentation which could be a subset of the certification package. It may be in the form of a technical document, technical letter, or annotated briefing. The information generally included as part of the accreditation package includes as a minimum:

- Executive summary of mission overview, architectural description, and system configuration, including interconnections

- Memorandum of Agreements (MOA)

- Waivers signed by the DAA that specific security requirements do not need to be met or are met by other means (e.g., procedures)

- Residual risk statement, including rationale for why residual risks should be accepted/rejected

- Recommendation for accreditation decision

Step 5 is optional and involves the DAA(s) or his/her representative (s) conducting a site accreditation survey to ensure the security requirements meet the requirements for the system. Final testing can be conducted at this time to ensure the DAA(s) are satisfied that the residual risk identified meets an acceptable level of risk to support its purpose. The activities include:

- Assess system information (this is the certification package review)
- Conduct site accreditation survey

Step 6 involves the DAA making the accreditation decision. This decision is based on many factors, such as global threats, system need/criticality, certification results and recommendations, residual risks, the availability or cost of alternative countermeasures, and factors that transcend security such as program and schedule risks, and even political consequences. The DAA has a range of options in making the accreditation decision, including the following:

- Full accreditation approval for its originally intended operational environment, including a recertification/reaccreditation timeline

- Accreditation for operation outside of the originally intended environment (e.g., change in mission, crisis situation, more restrictive operations)

- Interim (temporary) accreditation approval, identifying the steps to be completed prior to full granting of accreditation and any additional controls (e.g., procedural or physical controls, limiting the number of users) that must be in place to compensate for any increased risk

- Accreditation disapproval, including recommendations and timelines for correcting specified deficiencies

Step 7 involves maintaining the system accreditation throughout the system life cycle. Accreditation maintenance involves ensuring that the system continues to operate within the stated parameters of the accreditation. For example, that the stated procedures and controls of the system stay in place and are used, that the environment does not change outside of the stated parameters, that other types of users are not added to the system (e.g., users with lower clearances), that no additional external connections are made to the systems or that additional security requirements are not imposed on the system. Any substantial changes to the stated parameters of the accreditation may require that the system be recertified or reaccredited. It is important to note that recertification and reaccreditation activities may differ from those performed in support of a previous accreditation decision. For example, the system security mode of operation may change from system-high to compartmented mode, requiring more stringent security measures and an in-depth analysis of these measures. Applicable security policies/regulations, C&A team members, and/or DAA(s) may also change. Section 2.3 provides more information on events that affect system security that might require a system to be recertified or reaccredited.

2.2.1 Certification and Associated Security Disciplines

Certification activities and the associated results/recommendations are performed in support of the accreditation decision. Certification is a method for ensuring that an appropriate combination of system security measures are correctly implemented to counter relevant threats and vulnerabilities. That is, the certification effort must assess the effectiveness and interdependencies of security measures, as well as possible interferences or conflicts among them. These measures are typically based on the system security policy and operational requirements. It must be emphasized that in order to provide a realistic and effective analysis of the security posture of a system, all appropriate security disciplines (an INFOSEC perspective) must be included in the scope of the certification. For example, while a system may have very strong controls in one area (e.g., COMPUSEC), weak controls in another area (e.g., lax procedures) may undermine the systems overall security posture. The security disciplines to be considered include:

- COMPUSEC

- COMSEC

- Technical security (TECHSEC) (e.g. emission security, TEMPEST, tampering)

- Physical security

- Personnel security

- Administrative security

11

- • Others as appropriate (e.g., operations security (OPSEC), electronic security, signals security, transmission security (TRANSEC), cryptosecurity)

The concept and definitions (see appendix A) of some of these disciplines were developed at a time when security was viewed more as independent, loosely coupled disciplines, without an INFOSEC perspective to tie many of these various concerns together. In addition, the boundaries between the disciplines are unclear. Some disciplines are considered subsets of another; others are equivalent terms, but used by different communities of interest. While independent analyses of the security measures within a discipline may be done as part of the certification, the key is that the results of these analyses must be viewed together, not individually, to assess the overall security posture of the system.

Figure 2.2 illustrates one possible interrelationship of the security disciplines. The placement of the disciplines shows one possible overlap among the boundaries, and provides a categorization of the disciplines into three general areas: communications related, AIS related, or manual/information related. Depending on the particular system or environment, other relationships are possible. The remainder of this section presents a high-level overview of some representative security measures that may be appropriate for a given system for the first six disciplines listed above. The other disciplines will not be expanded in this section.

COMPUSEC measures may play an important role in mediating system risk. Certification activities include assessing the pervasiveness of these measures. For instance, the certification effort will determine whether the measures provide sufficient protection and whether they adequately enforce system security policies and requirements. How well these measures work in conjunction with or complement non-COMPUSEC measures must also be considered.

When computer equipment (e.g., workstation, hosts, and peripherals) is interconnected (e.g., via a local area network (LAN) or wide area network (WAN)), certification activities include assessing the protection, control, and adequacy of COMSEC measures. In this context, *interconnection* means the operational exchange of information among systems or within a system via data communications or networks. Certification will assess whether appropriate COMSEC policies and procedures are applied and approved equipment is used to counter threats and vulnerabilities of network components (e.g., packet switches, gateways, bridges, repeaters, transmission media).

Certification activities may include determining whether processing facilities or equipment comply with the appropriate national policy on compromising emanations.

For example, as part of certification, TEMPEST tests may be conducted, equipment installation or physical control space inspected, and encrypted/clear text (also known as Red/Black) separation procedures reviewed. The selection and evaluation of TEMPEST countermeasures are based on several factors such as data sensitivity level, amount of sensitive data, equipment used, and facility location.

A combination of physical security measures is needed to protect most systems. Consequently, certification activities often include inspecting the system in its operational environment/configuration to determine the adequacy of physical security measures. For some environments, a technical surveillance countermeasures (TSCM) survey may be conducted to identify exploitable technical and physical security vulnerabilities.

INFOSEC

Communications Related

AIS Related

COMSEC

Cryptosecurity

Emission Sec.

Electronic Sec.

Transmission Sec.

Technical Sec.

COMPUSEC

Data Sec.

Information Sec.

Administrative Sec.

Personnel Sec.

Environmental Sec.

Physical Sec.

Operations Sec.

Manual/Information Related

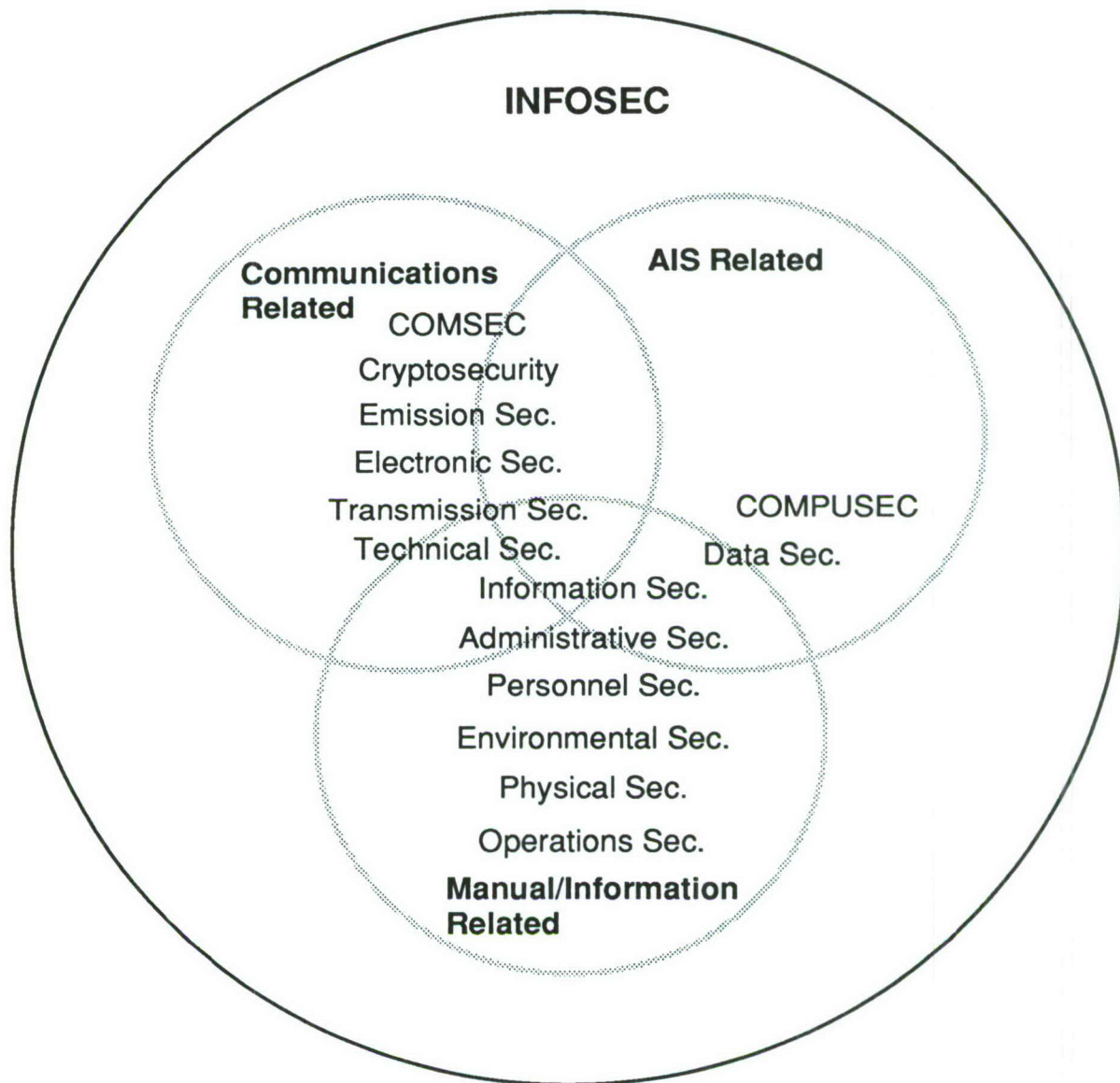Figure 2.2.   INFOSEC Security Discipline Interrelationship

Personnel security measures are also considered as part of system certification. Certification activities must ensure that personnel are appropriately cleared and/or approved for access to the system or portions thereof. Additionally, a determination of whether personnel security measures are commensurate with the overall risk index or

13

system security mode of operation (e.g., dedicated, system-high, compartmented, or multilevel) must be made.

Administrative security procedures are used in conjunction with or in lieu of automated measures. Certification activities include inspecting relevant documentation (e.g., *Trusted Facility Manual and Standard Operating Procedures*) to determine the adequacy of administrative controls and ensuring that the procedures are followed. Additionally, certification activities will verify that security personnel (e.g., information system security officers) have been appointed and that these individuals thoroughly understand their responsibilities for ensuring compliance with system security policies and procedures.

2.2.2 Factors That Influence the Certification Process

A number of factors may influence the determination of the C&A activities to be performed and the appropriate level of effort for those activities. While the high-level C&A process provides a uniform framework for performing C&A, more specific guidance is needed in order to apply the process to a given system in a specific environment or situation. This section briefly outlines some of the important factors that are key to tailoring the C&A process for a specific environment.

The security requirements that apply to a system are interpretations of generic requirements in the context of the system's mission, operational concept, and threat environment. C&A activities must be tailored to address the system's specific security requirements. For example, the C&A activities associated with a network whose mission is to deliver fixed format messages between the systems that use that network's services with assurances of message integrity and delivery within a set time will be different from those associated with a local-area network used by a collection of individual users for office automation.

The complexity of a system involves both the architectural complexity of the information system (i.e., the variety of components and functions) and the operational complexity of the total system (including user activities that perform the mission). Clearly, the depth of technical analysis and testing required for a local area network with workstations, file servers, and gateways to wide area networks is far greater than that needed for a stand-alone PC. The level of operational complexity will be primarily reflected in the evaluation of non-technical safeguards and in the risk analysis.

The risk environment in which the system operates (or is intended to operate) includes not only the sensitivity of the data the system handles and the clearances/authorizations of system users and external interfaces, but also the system criticality and the nature and level of the threats against it. C&A activities should be tailored to the level of potential risk associated with the system. For example, relatively little technical analysis may be required for a system that handles routine information and is not mission critical (e.g., office automation system).

The scope of C&A activities should depend on whether the system incorporates (a) previously evaluated products or (b) products or subsystems used in a system that has already been certified and accredited. The effort should be able to make use of C&A work done by other organizations. In addition, if inadequate attention has been paid to C&A up to some point in a system's life cycle, the C&A activities after that point will have to be tailored to compensate for prior inadequacies.

2.3 Recertification and Reaccreditation

Various recertification and reaccreditation cycles are currently prescribed. Typically these range between three and five years. For example, current DoD policy states that a system shall be reaccredited every three years, regardless of change [1]. On the other hand, Director of Central Intelligence (DCI) policy requires a five year reaccreditation cycle [6]. During this time, periodic reviews of the system should be conducted to ensure that no changes in the system have occurred that might necessitate reaccreditation before the three or five-year cycle.

Another reason for reaccrediting (and recertifying) a system is that major changes have been made to some aspect of the system that impacts security. The level of effort, in this case, for recertification and reaccreditation will depend on the certification factors (such as those described in section 2.2.2) as well as the possible impact of the changes made. In this situation, the recertification activities should concentrate on those aspects of the system that have changed since the original certification. The results of previous certification activities related to unchanged parts of the system will likely be able to be reused with no (or only minor) changes. The following is a partial list of events affecting system security that might require a system to be recertified and reaccredited:

- A change in criticality and/or sensitivity level that causes a change in the countermeasures required

- A change in the security policy (e.g., access control policy)

- A change in the threat or system risk

- A change in the activity that requires a different security mode of operation

- Additions or a change to the operating system or to software providing security features

- Additions or a change to the hardware that requires a change in the approved security countermeasures

- A breach of security, a breach of system integrity, or an unusual situation that appears to invalidate the accreditation by revealing a flaw in security design

15

- A significant change to the physical structure of the facility or to the operating procedures

- A significant change to the configuration of the system (e.g., a workstation is connected to the system outside of the approved configuration)

- For networks, the inclusion of an additional (separately accredited) system(s) or the modification/replacement of a subscribing system that affects the security of that system

- Results of an audit or external analysis

For systems with multiple accreditors, recertification and reaccreditation requirements and responsibilities should be identified in the MOA. For example, if a jointly accredited system is governed by the requirements of both DoDD 5200.28 [1] and DCI Directive (DCID) 1/16 [6], the DAAs, as part of their agreements documented in the MOA, should resolve the conflict in accreditation cycles.

SECTION 3

PRIMARY C&A ROLES

This section identifies the DAA and the certification agent as primarily responsible for the C&A of systems. The certification agent provides direct support to the DAA in making the accreditation decision. DoD component regulations define various security roles and responsibilities, and while the titles may vary, the responsibilities are similar.

In addition to the DAA and certification agent, the following roles are identified in this guideline as being key to the successful accreditation of some systems: Program Manager (PM), product vendors, systems integrator, systems engineers, and applications developer. Not all roles will be necessary for the C&A of all types of systems. The size, complexity, and status (e.g., new acquisition, upgrade, existing system) will determine the need for these additional roles. For example, accrediting a stand-alone PC will probably not require any effort from these additional roles. The following sections discuss the DAA, the certification agent/certification team, and other roles in terms of their responsibilities in the C&A process. Appendix B provides guidance on identifying the appropriate DAA for a given system.

3.1 DAA

By accrediting a system, the DAA formally assumes the responsibility for the operation of the system within a specified environment. The DAA must have the authority to allocate resources to achieve an acceptable level of security and to remedy security deficiencies. The accreditation decision shows that due care has been taken to balance security requirements, mission, and resources against a defined risk. More or less stringent security measures than those stated in applicable policies may be established by the DAA, if deemed appropriate. The accreditation decision also is a recognition by the DAA that an acceptable level of risk has been attained and that the DAA accepts the operation of this system under the stated parameters of the accreditation.

The DAA may delegate the authority to accredit systems; however, specific service/agency regulations need to be reviewed for guidance in this area. For example, Army Regulation (AR) 380-19 [7] policy states that for critically sensitive Army systems (i.e., systems that process any Top Secret data) operating in the dedicated, system-high, or partitioned modes, Major Command (MACOM) commanders may further delegate, in writing, accreditation authority to general officers or Senior

Executive Service personnel within their commands. Factors to consider before delegating accreditation authority are the resources available to the DAA and his or her supporting staff for realistically assessing the security posture of the system, both in technical expertise and clearance for or accessibility to the appropriate threat data.

The DAA will probably not be involved in day-to-day monitoring of the certification activities and in making many of the routine decisions regarding the system. Normally, the DAA appoints a representative(s) to act as a security focal point and to assist in making routine decisions, attending meetings, and providing coordination. While the DAA retains final responsibility to accredit the system, many of the accompanying duties will be delegated to this representative(s). The DAA representative(s) will actively coordinate with the certification agent (and PM, if applicable) to ensure that all security requirements are met and that all activities in support of accreditation are completed in accordance with procedures. All major decisions made during the system life cycle in support of the accreditation decision should be formally documented and coordinated with the DAA.

Some environments may require multiple DAAs to accredit the system. These environments can generally be divided into two types: (1) those systems requiring joint accreditation and (2) those systems composed of the interconnection of separately accredited systems. A working group, composed of individuals representing each of the accrediting organizations, may be necessary to resolve accreditation issues. The representative(s) for each of the DAAs responsible for the system accreditation are likely participants in this working group. The primary function of this group would be to ensure that all organizations involved understand the conditions and major agreements affecting the system accreditation, and that these conditions and agreements are documented in an MOA. The definition of the security requirements and the assignment of security responsibility among the involved organizations are examples of the types of decisions to be documented. The following sections provide additional information on identifying the DAA in these two types of systems.

3.1.1 Joint Accreditors

Some types of systems that will be accredited as a single system might require multiple accreditors. Examples include the following:

- A system that processes different types of information (e.g., cryptologic, Sensitive Compartmented Information (SCI), or Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI))

- A system used by multiple data owners who process the same type of information

- A system supporting multiple organizations (where the DAAs from each organization will be responsible for collectively accrediting the system)

18

- A system connected to a backbone network (where the system (e.g., host system) accreditor and the network accreditor jointly accredit the system as a whole)

Joint accreditation occurs when different components of the overall system come under the jurisdiction of different DAAs, and the responsible DAAs collectively accredit the system.

Systems that have joint accreditors require additional planning and coordination to ensure that all parties involved have a common understanding of their responsibilities in the C&A process, the risks involved, and the security posture of the system. When a system is to be jointly accredited, the roles and responsibilities of the DAA(s), certification agents, and other key security roles of all participating organizations must be clearly defined and documented. An MOA should be used to identify security responsibilities and to document all agreements made. In addition, the requirements for the system and the criteria used to accredit the system should be clearly documented. C&A milestones should be coordinated with the DAA(s) and their representatives, and documented in C&A planning documents.

3.1.2 Multiple Accreditors

When separately accredited systems managed by different DAAs are interconnected, negotiation must occur among the DAAs to address the interconnection requirements of each system involved. MOAs are required when systems interconnect, for example, within their own sponsoring agency/service, with another agency, or with government contractors. An MOA documents the results of the negotiations, forming an agreement signed by the participating DAAs. Each DAA must, therefore, carefully examine the additional potential risks imposed on the system by connecting to other systems. Additional certification activities may be required to determine the security posture of the overall systems before the separately accredited systems may be interconnected.

In some cases, the agreement for interconnection is among peer organizations. In this situation, the MOA will formalize the agreement among the DAAs on the division of responsibilities and the criteria used to accredit each system. The MOA should include, at a minimum, the following information:

- Classification range of data maintained on or transmitted between systems

- Clearance level(s) of the users

- Intended use of the system

- Identification of the authority to resolve conflicts among the DAAs

- Countermeasures to be implemented prior to interconnection

- Statements of accreditation of each interconnected system

- Procedures for notification of changes in the system

- Procedures for notification of proper parties in case of security violations

- Accreditation criteria

- Recertification/reaccreditation requirements and responsibilities

In other cases, when identifying the DAA(s) for a given system, consideration must be given to interconnections separately accredited multiuser telecommunications networks. Special consideration must be given to additional risks when connecting to networks because of the potential exposure of data in the system to the larger community of network users. The DAA(s) must consider the security posture of each network component, in addition to their individual systems, before accepting the risk of connecting to other systems. In addition, the accreditor(s) of these networks may require C&A documentation from the subscriber system before allowing interconnection.

3.2 Certification Agent/Certification Team

The certification agent is the individual(s) responsible for making a technical judgment of the systems compliance with stated requirements and to identify and assess the risks associated with operating the system. In addition, the certification agent has the responsibility for coordinating the various activities of the certification process and merging all the pieces of the final accreditation package that will be presented to the DAA. Although the fundamental role of the certification agent does not differ among certification efforts, the activities and level of effort required may vary (see section 2.2.2).

Some characteristics, such as technical expertise, impartiality (i.e., unfair bias toward achieving a particular result), and objectivity (i.e., minimum subjective judgment or opinion) are important considerations when selecting the appropriate certification agent. In general, certification activities should be performed by competent technical personnel in cooperation with but as independent of the system developer and the PM as possible.

The certification team is the collection of individuals and/or organizations involved in some aspect of the certification process. Given the increasing complexity of many AISs and the wide variety of security disciplines that must be assessed during certification, most organizations do not have adequate or appropriate in-house resources to perform many of the required certification activities (e.g., product evaluations, testing). To perform some of these activities, the certification agent may rely on the resources of other organizations that have the specialized skills necessary (e.g., TEMPEST).

3.3 Other Security Roles

Although the PM is not typically responsible for performing daily security activities, the PM is responsible for seeing that they are implemented. The PM has the responsibility for the overall procurement, development, and possibly operation of the system, and must coordinate all security-relevant portions of the program with the DAA and the certification agent. The PM provides the resources, coordinates the scheduling of security milestones, and determines priorities. The PM should not be (or should not be above) the DAA, as this may place security subordinate to the programs cost, schedule, and performance imperatives.

Depending on the type of system and the type of program (e.g., development effort, COTS acquisition, system upgrade), other roles will be involved in the overall security of the system, from requirements definition through operations and maintenance. System integrators, systems engineers, security engineers, application developers, product vendors, the independent verification and validation (IV&V) assessors, and others may be responsible for addressing security concerns during system development, including activities such as specifying requirements, testing, reviewing documentation, developing procedures, conducting installations, and performing component evaluations.

For some systems (e.g., a large acquisition, a complex distributed system), an information system security working group (ISSWG) may be necessary to direct security activities and identify/resolve security-related issues throughout the system development life cycle and operation of the system. The ISSWG may include the DAAs representative, whose role is to identify, address, and coordinate security accreditation issues with the DAA. The ISSWG normally manages and performs security-related activities that include identifying and interpreting security regulations and standards, preparing and/or reviewing security portions of the Request for Proposal (RFP), overseeing major acquisition strategy decisions, and managing C&A issues. Ideally, the technical security representatives from or consultants to the appropriate participating service or agency organizations should be involved in these activities. These participants serve as security consultants to the PM throughout the entire acquisition life cycle.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 4

SECURITY POLICY

4.1 Current Security Policy

Security policy exists at different levels of abstraction. Federal- and national-level policy is stated in public laws, Executive Orders (EOs), National Security Directives (NSDs), National Security Telecommunications and Information Systems Security (NSTISS) issuances, Federal Information Processing Standard Publications (FIPS PUBS), Office of Management and Budget (OMB) circulars, and other resources. DoD-level policy includes DoD directives, regulations, and standards that implement the National-level policy and set additional requirements. Similarly, service and agency policies further interpret the DoD and national-level policies, as appropriate, and may also impose additional requirements. Together with mission specific security requirements, the collection of these policies can be used to produce a system security policy. A system security policy comprises a comprehensive presentation of the system derived from national/federal level policy, local policy, and mission specific security requirements. The security policy for a system should be well defined at the beginning of the system life cycle and must be considered throughout each phase. Figure 4.1 illustrates the partial hierarchy of policies and guidance. The national and federal policies apply to both civil and defense agencies; however, individual civil agency policies are not listed in this document. Defense policies are listed, in part, in Appendix C.

Current security policy does not reflect the evolving perspective of system security as an interdependent, cohesive collection of security disciplines. At the DoD and component levels, separate policies exist for each discipline (or set of related disciplines), adding to the proliferation of policy. As a result, the policies applicable to a given system are sometimes not well coordinated or consistent. The following sections briefly highlight the key national- and DoD-level security policy.

4.1.1 National Security Policy

National Policy for the Security of National Security Telecommunications and Information Systems provides initial objectives, policies, and an organizational structure to guide the conduct of activities directed toward safeguarding systems that process or communicate national security information [8]. It is intended to assure full participation and cooperation among the various existing centers of technical

23
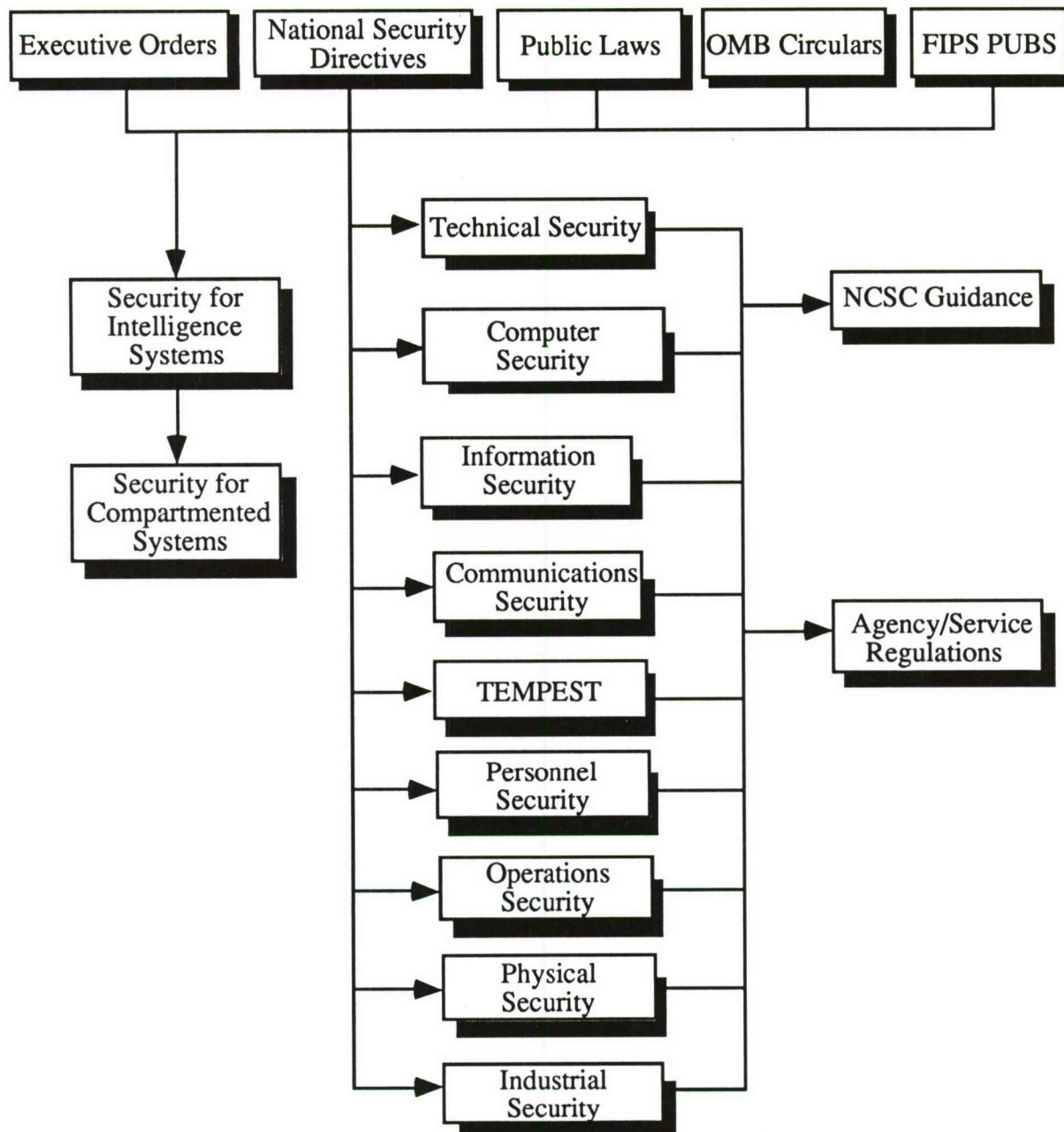
Figure 4.1   Information Security Policy and Guidance[1]

expertise throughout the executive branch. It assigns the Director, NSA, as the
National Manager for NSTISS, responsible to the Secretary of Defense as Executive
Agent for carrying out assigned responsibilities. Among the assigned responsibilities

---

[1]The figure is not meant to imply that the policies represented in the top boxes are of equal authority; they
are not. The figure only intends to show that these higher level policies influence the
department/service/agency issuances.

is to act as the government focal point for cryptography, telecommunications systems security, and information systems security.

EO 12356, *National Security Information*, prescribes a uniform system for classifying, declassifying, and safeguarding national security information [9]. Although the public should be informed of the activities of its government, the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this EO unless its disclosure reasonably could be expected to cause damage to the national security.

EO 12333, *United States Intelligence Activities*, directs the DCI, as one responsibility, to ensure the establishment by the Intelligence Community (IC) of common security and access standards for managing and handling foreign intelligence systems, information, and products. [10]

OMB Circular No. A-130, *Management of Federal Information Resources*, establishes policy for the management of federal information resources [11]. The term information resources management means the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology. The policies established in this circular apply to the information activities of all agencies of the executive branch of the federal government. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives.

FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, a national-level document, provides guidance to managers and technical staff in establishing and carrying out a program for C&A of sensitive computer applications [12]. It identifies and describes the steps involved in performing C&A, the important issues in managing a C&A program, and the principal functional roles needed within an organization to carry out such a program. The FIPS PUB 102 guidance applies to all federal agencies and departments.

The *Computer Security Act of 1987*, also known as Public Law 100-235, creates a means for establishing minimum acceptable security practices for improving the security and privacy of sensitive unclassified information in federal computer systems [13]. This law assigns responsibility to the National Institute of Standards and Technology (NIST) for developing standards and guidelines for federal computer systems processing unclassified data. However, the **Warner Amendment** (section 2315 of title 10, United States Code) exempts AISs processing sensitive unclassified information if the function, service, or use of the system (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves the command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapon system, or (5) is critical to the direct fulfillment of military or intelligence missions. The law also requires establishment of security plans by all operators of federal computer systems that contain sensitive information.

4.1.2 DoD/DCI Security Policy

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, the high-level security policy, sets the security requirements for AISs within the DoD [1]. The directive assigns responsibility to the heads of DoD components to assign official(s) as the DAA responsible for accrediting each AIS under his or her jurisdiction and for ensuring compliance with the AIS security requirements. The DAA is responsible to review and approve security safeguards of AISs and issue accreditation statements for each AIS under the DAAs jurisdiction based on the acceptability of the security safeguards for the AIS. Enclosure 3 of this directive sets minimum security requirements that must be met through automated or manual means in a cost effective, integrated manner. Enclosure 4 of this directive describes a procedure for determining the minimum AIS computer-based security requirements based on the system security mode of operation, user clearance levels, and classification of data in the AIS. Enclosure 5 recommends using the Trusted Network Interpretation (TNI) of the *Trusted Computer System Evaluation Criteria in Specific Environments* for evaluating networks [14]. The TNI provides guidance for the specification, development, evaluation, and acquisition of trusted networks.

Issued under the authority of DoDD 5200.28 are DoD 5200.28-M, *Automated Information System Security Manual* [15], and DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria* [2]. DoD 5200.28-STD provides a set of criteria against which the security features of a product may be evaluated. There is currently a joint NSA/NIST effort to produce the Federal Criteria, as an eventual replacement to DoD 5200.28-STD.

DCID 1/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, and its supplement apply to all IC agencies, all other U.S. Government departments and agencies, and allied governments processing U.S. intelligence information [6]. The directive establishes the minimum administrative, environmental, and technical security requirements for the allowed operating modes of all applicable AISs (e.g., AISs, separately accredited networks and connected AISs, and PCs). Additional security measures may be established by the accrediting authority. It also defines the accreditation and reaccreditation responsibilities and procedures applicable to AISs processing intelligence information.

Although DoDD 5200.28 and DCID 1/16 are the key security directives, they primarily focus on COMPUSEC. The C&A process must consider the spectrum of security measures, including administrative, physical, environmental, personnel, COMSEC, emissions, and technical security.

4.2 Policy Related Issues

As discussed in section 4.1, a multitude of security policy documents exist. This proliferation of policy makes it difficult for the responsible security personnel to keep

up with changes in policy and to be aware of all the applicable policies for a given system. The problem increases when different service/agency systems are interconnected; in those cases, the policies relevant to all involved components may then be applicable. On the other side, the rapid advancement of technology and the required streamlining and consolidation of efforts are forcing a reexamination of current policy. This section highlights some of the C&A-related issues that this series of documents are attempting to, at least partially, address.

4.2.1 Rapid Technology Changes

Rapidly changing technology has made it difficult for policy to keep up with new security challenges brought about by advances in capabilities and technology. For example, current policy provides little guidance for the range of systems that span large, central computer facilities to stand-alone PCs or intelligent workstations often tied together over LANs or connected via complex networks. These systems have significant differences in functionality and vulnerabilities, and current policy provides little guidance to DAAs on determining an acceptable level of risk based on the technology, environmental factors, and operational requirements. Improved guidance is needed on how to certify and accredit all types of systems: networks, distributed systems, systems with integrated workstations, database management systems (DBMSs), and multilevel secure (MLS) systems. Differences among component policies also cause difficulties as many individually certified and accredited systems from multiple components are being integrated into a larger system.

4.2.2 Planning for C&A

Determining a reasonable and realistic level of effort for certification (and recertification) is key to a successful accreditation. The analysis, evaluation, and testing requirements to support certification may require substantial commitments of resources that must be planned for early in the system life cycle (for example: as part of the RFP). However, in some cases, for example an environment needing a low assurance system, the benefit of spending any additional resources for certification may be questionable. For example, in an acquisition of COTS products (e.g., database management system (DBMS)) (assuming the requirements stated met the need), a determination must be made regarding how much, if any, additional evaluation and testing is necessary outside of the acceptance testing normally associated with the acquisition. In many cases, the functionality and security attributes of COTS products are well known and documented, and perhaps only the operating environment in which the COTS product will be used must be evaluated. As another example, a reasonable and justifiable effort (both in time and dollars) for certifying a dedicated or system-high system operating in a secure environment should be determined.

4.2.3 Certification Boundaries

Encryption has become an increasingly common component in systems, and better guidance is needed for determining when COMSEC or COMPUSEC criteria are applicable in a given system. In some cases, the AIS will have to be examined by NSA (the responsible authority for COMSEC) to make informed COMSEC decisions. In other cases, an approved embedded COMSEC component (e.g., an encryption chip on a board in a PC) may not require a separate COMSEC evaluation. In these cases, configuration management of the AIS must also consider COMSEC.

Another area with little guidance available concerns the use of the results of product/component evaluations (e.g., products on the Evaluated Products List (EPL), Preferred Products List (PPL), Degausser Products List (DPL) [16]) or other evaluations (e.g., DMS component deployment approval) as input to a system certification. In some cases, those evaluation results are used as substitutes for system certification. For example, a component deployment approval (as done by Defense Information Systems Agency (DISA) as part of the DMS component approval process) merely certifies that the AIS (or component) properly implements the message-handling requirements. It does not supplant the need for overall system certification.

As the number and complexity of networks and distributed systems increase, the confusion over areas of responsibility for the components of the system also increases. Various authorities will have responsibility for different components, such as the actual communications components (e.g., communications lines, switches, routers), host computers, shared devices on the network (e.g., printers, servers), and the end-user terminals or workstations. During the certification of these complex systems, the boundaries of each of the components and the responsibility for certification of each area must be clearly defined to ensure that the entire system is covered in the effort, as well as ensuring that the entire system is viewed as a whole.

4.2.4 Acceptable Level of Risk

Part of the accreditation decision is the acceptance of a given level of risk against a defined threat. In order to make an informed decision, the DAA must be aware of both the definition of risk and the identification of the specific threat as it applies to the system being considered for accreditation. The DAA must balance (1) the risk of disclosure, loss, or alteration of information; (2) the availability of the system based on the vulnerabilities identified by the certification process; (3) the threat that these vulnerabilities may be exploited in the specific environment in which the system is being used; and (4) the operational need and benefits.

In addition, there may be situations where the DAA must balance the risk against operational requirements mandating acceptance of higher risk, such as during a crisis situation. While operational needs can dramatically change during a crisis, the need for security is even more critical during these times. For example, in a crisis situation,

perhaps tightened procedural and physical controls and the removal of connections to users in less secure areas could compensate for the increased risk of connecting the systems.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

TERMINOLOGY

Key C&A terms are defined herein. Numerous national, DoD, and service/agency policies were consulted in defining these terms. Existing national or DoD-level definitions were used, as appropriate. Where necessary, discussion paragraphs are included to expand on a definition in an attempt to clarify possible ambiguities in its interpretation.

Accreditation

Formal declaration by a designated approving authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Note: Accreditation is the formal declaration by a DAA that a system is approved to operate: (a) in a particular security mode; (b) with a prescribed set of countermeasures (e.g., administrative, physical, personnel, COMSEC, emissions, and computer security controls); (c) against a defined threat and with stated vulnerabilities and countermeasures; (d) within a given operational concept and environment; (e) with stated interconnections to other systems; (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility; and (g) for a specified period of time.

Accreditation Package

A product of the certification effort and the main basis for the accreditation decision.

Note: The accreditation package, at a minimum, will include a recommendation for the accreditation decision and a statement of residual risk in operating the system in its environment. Other information included may vary depending on the system and/or the DAA.

Administrative Security

The management constraints and supplemental controls established to provide protection for a system. Synonymous with **Procedural Security**.

Note: Examples include operational procedures (e.g., how to shut down the system securely), administrative procedures (e.g., granting access to a computer facility), and accountability (e.g., audit procedures for the system administrator to follow).

AIS Security

Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by an AIS.

Assurance

A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Note: Assurance refers to a basis for believing that the objective and approach of a security mechanism or service will be achieved. Assurance is generally based on factors such as analysis involving theory, testing, software engineering, validation, and verification. Life-cycle assurance requirements provide a framework for secure system design, implementation, and maintenance. The level of assurance that a development team, certifier, or accreditor has about a system reflects the confidence that they have that the system will be able to enforce its security policy correctly during use and in the face of attacks. Assurance may be provided through four means: (1) the way the system is designed and built, (2) analysis of the system description for conformance to requirement and for vulnerabilities, (3) testing the system itself to determine its operating characteristics, and (4) operational experience. Assurance is also provided through complete documentation of the design, analysis, and testing.

Audit

An independent review and examination of the records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Trail

A chronological record of system activities to enable the reconstruction, and examination of the sequence of events and/or changes in an event.

Authentication

A security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Authenticity

The service that ensures that system events are initiated by and traceable to authorized entities. It is composed of authentication and nonrepudiation.

Automated Information System (AIS)

Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data, and includes computer software, firmware, and hardware.

Note: The term "AIS" includes stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid;

32

associated peripheral devices and software; process control computers; security components; embedded computer systems; communications switching computers; PCs; workstations; microcomputers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, as may be developed.

Availability
The property of being accessible and usable upon demand by an authorized entity.

Baseline
A set of critical observations or data used for a comparison or control.

Note: Examples include a baseline security policy, a baseline set of security requirements, and a baseline system.

Category
A restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data.

Note: Examples include SCI, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special categories of information only after being granted formal access authorization.

Certification
The comprehensive analysis of the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements.

Note: Certification is done in support of the accreditation process and targets a specific environment. Certification includes risk analysis, security testing, and evaluations, as well as other activities, as needed.

Certification Agent
The individual(s) responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certification and Accreditation Plan
A plan delineating objectives, responsibilities, schedule, technical monitoring, and other activities in support of the C&A process.

Certification Package
A product of the certification effort documenting the detailed results of the certification activities.

Note: The contents of this package will vary depending on the system.

Classified Information
National security information that has been classified pursuant to Executive Order 12356.

Communications Security (COMSEC)
Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such communications.

Note: COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC materials.

Component
Any of the constituent parts of a system.

Note: A component may be a small element of a system or the whole system. It can be physical (e.g., circuit board), logical (e.g., software routine), or support personnel.

Computer
The hardware, software, and firmware components of a system that are capable of performing calculations, manipulations, or storage of data. It usually consists of arithmetic, logical, and control units, and may have input, output, and storage devices.

Computer Security (COMPUSEC)
Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management
The management of features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of a system throughout the development and operational life of the system.

Contingency Plan
A plan maintained for emergency response, backup operations, and post-disaster recovery for a system, as part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Countermeasure
Any action, device, procedure, technique, or other measure that reduces a risk or a vulnerability.

Covert Channel
An unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates a system security policy.

Note: Covert channels may be storage or timing channels. A covert storage channel involves the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. A covert timing channel is one in which one process signals information to another process by modulating its own use of system resources in such a way that this manipulation affects the real response time observed by the second process.

Cryptosecurity
The component of COMSEC that results from the provision of technically sound cryptosystems and their proper use.

Data Security
The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Designated Approving Authority (DAA)
The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Note: FIPS PUB 102 uses the term "Accrediting Official" for the DAA [12]. "Accrediting Authority" is another term used. The DAA must have the authority to evaluate the overall mission requirements of the system and to provide definitive directions to system developers or owners relative to the risk in the security posture of the system. Generally, the more sensitive the data processed by a system, the more senior the DAA. A DAA may be responsible for several systems, and each system may have a single or multiple DAAs. When there are multiple accreditors, the sharing of responsibilities must be carefully defined in an MOA.

DoD Component
Refers to the Office of the Secretary of Defense (OSD), the Military Departments and Services within those departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the unified and specified commands, the defense agencies, and the DoD field activities.

Electronic Security
Protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the interception and analysis of non-communications electromagnetic radiations, such as RADAR.

Emission Security
Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment, AISs, and telecommunications systems.

Endorsement
 NSA approval of a commercially developed telecommunications or AIS protection equipment or system for safeguarding national security information.

Environment (System)
 The aggregate of procedures, conditions, and objects that affects the development, operation, and maintenance of a system.

 Note: Environment is often used with qualifiers such as computing environment, application environment, or threat environment, which limit the scope being considered.

Evaluation
 The technical analysis of a component's, product's, subsystem's, or system's security that establishes whether or not the component, product, subsystem, or system meets a specific set of requirements.

Exception
 With respect to C&A, an exception indicates the implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirements may be used for a specified period of time. (see **Waiver**)

Formal Access Approval
 Documented approval by a data owner to allow access to a particular category of information.

Implementation
 The phase of the system development process in which the detailed specifications are translated into actual system components.

Information Security
 The result of any system of policies and procedures for identifying, controlling, and protecting, from unauthorized disclosure, information that requires protection.

Information System
 Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data, and includes software, firmware, and hardware.

Information Systems Security (INFOSEC)
 The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Note: The term "INFOSEC," as it applies to this concept of the totality of security applied to a system, has evolved. This series of documents will use the term INFOSEC--Information Systems Security--to reflect that concept of the totality of system security.

Information Systems Security Products and Services Catalogue (INFOSEC Catalogue) (also referred to as the Products and Services Catalogue) [16]

A catalogue issued by NSA that incorporates several security product and services lists. It is available through the Government Printing Office. Some of the lists included in the catalogue are the following:

Degausser Products List (DPL) - a list of commercially produced degaussers that have been evaluated against specific requirements for the erasure of classified data from magnetic media.

Endorsed Cryptographic Products List - a list of products that provide electronic cryptographic coding (encrypting) and decoding (decrypting), and which have been endorsed for use for classified or sensitive unclassified U.S. Government or Government-derived information during its transmission.

Endorsed Tools List (ETL) - a list of those formal verification systems recommended by the National Computer Security Center (NCSC) for use in developing highly trusted systems.

Evaluated Products List (EPL) - a documented inventory of equipment, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD.

Protected Network Services List - a list of the names and points of contact for commercial carriers providing government-approved "protected services" for your communications. The companies listed offer protection service (e.g., bulk trunk encryption) rather than a product.

NSA Endorsed Data Encryption Standard (DES) Products List - a list of cryptographic products endorsed by NSA as meeting Federal Standard 1027 [17]. These DES products have been endorsed for use in protecting U.S. Government or U.S. Government-derived unclassified sensitive information during transmission. They may not be used to secure classified information.

Off-Line Systems - a description of a variety of off-line capabilities that NSA can provide to meet customer requirements. Off-line refers to those cryptosystems for which encryption and decryption are performed separately from the transmitting and receiving functions.

Preferred Products List (PPL) - a list of telecommunications and information-processing equipment and systems that conform to the current national TEMPEST standard.

Integration

The synthesis of a system's components to form either larger components of the system or the system itself.

Integrity

Data integrity is that attribute of data relating to the preservation of (a) its meaning and completeness, (b) the consistency of its representation(s), and (c) its correspondence to what it represents.

System integrity is that attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Interim Approval

The temporary authorization granted by the DAA for a system to process information in its operational environment based on preliminary results of a security evaluation of the system.

Note: Interim approval allows the activity to meet its operational requirements for a given period of time while further assessing and improving its security posture. It gives the DAA the needed latitude to approve operational implementation of individual components of a system as they develop. Final approval is mandatory before full implementation.

Mission

A specific task with which a person, or group of individuals, or organization is entrusted to perform.

Mission Criticality

The property that data, resources, and processes may have, which denotes that the importance of that item to the accomplishment of the mission is sufficient to be considered an enabling/disabling factor.

Mode of Operation (Security Mode)

Description of the conditions under which a system operates, based on the sensitivity of data processed and the clearance levels and authorizations of the users.

Note: The DAA accredits a system to operate in a given mode of operation. Inherent in each of the five security modes (dedicated, system high, compartmented, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the system. Modes of operation are part of a paradigm based on confidentiality (information disclosure policy.) The applicability and/or usefulness of these modes of operation to a system whose principal security objective was integrity or availability is unclear.

Compartmented Mode: Security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following:

  a. Valid security clearance for the most restricted information processed in the system

  b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access

  c. Valid need-to-know for information to which a user is to have access

Dedicated Mode: Security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

  a. Valid security clearance for all information within the system

  b. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs)

  c. Valid need-to-know for all information contained within the system

Note: When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Multilevel Security: Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Partitioned Security Mode: Security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the system.

Note: This security mode encompasses the compartmented mode and applies to non-intelligence DoD organizations and DoD contractors.

System High Mode: Security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

  a. Valid security clearance for all information within the system

b. Formal access approval and signed non-disclosure agreements for all of the information stored and/or processed (including all compartments, subcompartments and/or special access programs)

c. Valid need-to-know for some of the information contained within the system

Need-to-Know
Access to, or knowledge or possession of, specific information required to carry out official duties.

Network
A communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Network Security
Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

Note: Network security includes providing for data integrity.

Non-Repudiation
Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Operations Security (OPSEC)
A process denying to potential adversaries information about capabilities and/or intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.

Penetration Testing
Security testing in which the evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

Note: The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under no constraints other than those applied to ordinary users or implementors of untrusted portions of the component.

Personnel Security
The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

Physical Security
The application of physical barriers and control procedures as countermeasures against threats to resources and sensitive information.

Procedural Security
See **Administrative Security**.

Product
A package of software, firmware, and/or hardware providing functionality designed for use or incorporation within a multiplicity of systems.

QUADRANT
Short name referring to technology which provides tamper-resistant protection to crypto-equipment.

Reaccreditation
The official management decision to continue operating a previously accredited system.

Note: Reaccreditation occurs (1) periodically, regardless of system change (based on policy (e.g., DoDD 5200.28 requires a 3 year reaccreditation cycle)) or (2) if major changes have been made to some aspect of the system that impact security.

Recertification
A reassessment of the technical and nontechnical security features and other safeguards of a system made in support of the reaccreditation process.

Note: The level of effort for recertification will depend on the nature of changes (if any) made to the system and any potential changes in the risk of operating the system (e.g., changes in the threat environment may affect the residual risk).

Residual Risk
The portion of risk that remains after security measures have been applied.

Risk
A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.

Note: Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

Risk Analysis
Process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses), and using the analysis as a basis for identifying appropriate and cost-effective measures.

Note: Risk analysis is a part of risk management, which is used to minimize risk by specifying security; measures commensurate with the relative values of the resources to be protected, the vulnerabilities of those resources, and the identified threats against them. The method should be applied iteratively during the system life cycle. When applied during the implementation phase or to an operational system, it can verify the effectiveness of existing countermeasures and identify areas in which additional measures are needed to achieve the desired level of security. There are numerous risk analysis methodologies and some automated tools available to support them.

Risk Assessment
Synonymous with **Risk Analysis**.

Risk Management
The process concerned with the identification, measurement, control, and minimization of security risk in information systems.

Note: Risk management encompasses the entire system life cycle and has a direct impact on system certification. It may include risk analysis, cost/benefit analysis, countermeasure selection, security test and evaluation, countermeasure implementation, and systems review. Enclosure 3 of DoDD 5200.28 mandates a risk management program be in place for each AIS to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.

Security
Establishment and maintenance of protective measures intended to ensure a state of inviolability from hostile acts and influences, design deficiencies, system/component failure/malfunction, or unintentional misuse.

Security Architecture
A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Note: A security architecture is basically an architectural overlay that addresses security. It is increasingly important in distributed systems, since there are many ways in which security functions can be distributed and care is needed to ensure that they work together.

Security CONOPS
A high-level description of how the system operates and a general description of the security characteristics of the system, such as user clearances, data sensitivity, and data flows.

Security Policy
The set of laws, rules, and practices that regulate how sensitive or critical information is managed, protected, and distributed.

Note: A security policy may be written at many different levels of abstraction. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; system security policy defines the rules and practices within a specific system; and technical security policy regulates the use of hardware, software, and firmware of a system or product.

Security Requirements
Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Security Safeguards
Protective measures and controls that are prescribed to meet the security requirements specified for a system.

Note: Safeguards may include security features as well as management constraints, personnel security, and security of physical structures, areas, and devices.

Security Test and Evaluation (ST&E)
An examination and analysis of the safeguards required to protect a system, as they have been applied in an operational environment to determine the security posture of that system.

Security Testing
A process used to determine that a system protects data and maintains functionality as intended.

Note: Security Testing may include hands-on functional testing, penetration testing, and verification.

Security Working Group
A group, representing various organizational entities, that meets to discuss security issues throughout a system's life cycle.

Note: Identification of security issues and suggested solutions are outputs of the group.

Sensitive Information
Information designated to require protection because its unauthorized disclosure, alteration, loss, or destruction could cause damage.

Note: It includes both classified and sensitive unclassified information.

Sensitive Unclassified Information
Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C Section 552a (the Privacy Act) [18], but that has not been specifically authorized under

43

criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Note: Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (Public Law 100-235) [13].

Sensitivity
The characteristic of a resource which implies its value or importance, and may include its vulnerability.

Note: As an example, the DoD uses a set of hierarchically ordered sensitivity levels (i.e., Confidential, Secret, Top Secret) to indicate the sensitivity of data. In addition, in many environments, labels such as Procurement Sensitive, Investigations, Medical, Payroll, or Project XYZ are used to refer to specific sets of information.

Signals Security
Generic term encompassing COMSEC and electronic security.

Subsystem
A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system.

System
A collection of components that may include computer hardware, firmware, software, data, procedures, environment, and people, so related as to behave as an interacting or interdependent unit.

Note: A system has a particular purpose and operational environment. A system may contain one or more components, subsystems, or products. The operational environment may encompass the computing facility or the site installation.

System Life Cycle
The duration of time that begins with the identification of a need to place a system into operation; continues through the system's design, development, implementation and operation; and ends with the system's disposal.

System Security Plan
A description of the risks, system security requirements, and how the system will meet the security requirements.

Systems Security Engineering
The efforts that help achieve maximum security and survivability of a system during its life cycle and interface with other program elements to ensure security functions are effectively integrated into the total systems engineering effort.

Technical Security (TECHSEC)

Equipment, components, devices, and associated documentation or other media that pertain to cryptography, or to security of telecommunications and AISs.

TEMPEST

A short name referring to investigation, study, and control of compromising emanations from telecommunications and AIS equipment.

Testbed

A system representation consisting partially of actual hardware and/or software and partially of computer models or prototype hardware and/or software.

Threat

Capabilities, intentions, and attack methods of adversaries to exploit any circumstance or event with the potential to cause harm to information or an information system.

Transmission Security (TRANSEC)

The component of COMSEC that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Trust

Confidence that an entity, to which trust is applied, will perform in a way that will not prejudice the security of the user of the system of which that entity is a part.

Note: Trust is always restricted to specific functions or ways of behavior (e.g., "trusted to connect A to B properly"). Trust is meaningful only in the context of a security policy; an entity may be trusted in the context of one policy, but untrusted in the context of another policy.

Trusted Computer System

A system that employs sufficient hardware, firmware, and software assurance measures to exhibit correct behavior in terms of operations defined by its security policy.

Trusted Computing Base (TCB)

Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.

Note: The ability of a TCB to enforce correctly a unified security policy depends on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Type Accreditation

Official authorization by the DAA to employ a system in a specified environment.

Note: Type accreditation includes a statement of residual risk, delineates the operating environment, and identifies specific use. It may be performed when multiple copies of a system are to be fielded in similar environments.

Unclassified Information

Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost, or susceptibility to fraud, waste, or abuse.

User

Person or process accessing a system by direct connections (e.g., via terminals) or indirect connections.

Note: "Indirect connections" relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

Verification

The process of comparing two levels of a system specification for proper correspondence or of proving that some property of a specification is correctly implemented by the system (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code).

Note: Verification may be formal or informal, or automated or not automated. Formal verification is the process of using formal proofs (complete mathematical argument) to demonstrate the consistency between formal specification of a system and formal security policy model (design verification) or between formal specification and its high-level program implementation (implementation verification). Formal implies using a formal mathematical language.

Vulnerability

A weakness in an information system or component (e.g., security procedures, hardware design, internal controls) that could be exploited.

Waiver

With respect to C&A, a waiver implies that a security requirement has been set aside and need not be implemented at all. (See **Exception**.)

APPENDIX B

Identifying The Appropriate DAA

The DAA for a given system is determined based on several factors: the type of information processed (e.g., SCI, SIOP-ESI, collateral), the office of primary responsibility (owner) of the system, and interconnections with separately accredited networks or systems. For some types of information, a single accrediting authority exists (the data owner), regardless of the system owner. However, for other information, the accreditor is determined primarily by the owner of the system. For example, in a system processing collateral information, the services/agencies may accredit the system.

In addition, the applicable security policies for a given system depend on the accrediting authority. A high-level mapping from the identified DAA for a system to the applicable security policies can be made. When a system has a single DAA, this mapping is simple. The DAA is generally aware of the appropriate service/agency (and DoD-level) policies that govern the system under his or her jurisdiction. However, when multiple DAAs are involved, this mapping of DAA to applicable policies can be more complex. When the DAAs are from other organizations, in particular from other services/agencies, the responsible individuals cannot be expected to be aware of the governing policies from other organizations. Systems that come under the responsibility of multiple accreditors may be subject to the requirements from the policies of all participating organizations. These policies must be clearly identified and documented (in the MOA) early in the C&A process.

Tables B-1 and B-2 identify the appropriate DAA and applicable policies for the services/ agencies. Service/agency policies should be consulted for details about authority to delegate accreditation responsibilities. Before connecting to a separately accredited network, the DAA of the system requesting connection must consider the additional risks of operation associated with connection. In addition, the DAA of the network will need to consider the security posture of the system requesting connection before allowing a connection to be made. The requesting system will have to comply with any additional security requirements of the network system before interconnecting. Table B-3 identifies the applicable policies, security mode of operation, and DAA(s) for the following separately accredited networks. Tables B-1, B-2, and B-3 appear at the end of this appendix.

- AUTODIN/DMS

- Military Network (MILNET)

- Defense Secure Network 1 (DSNET1)

- Defense Secure Network 2 (DSNET2) or the Top Secret WWMCCS Information Network Computer System (WINCS)

- Defense Secure Network 3 (DSNET3) or the Sensitive Compartmented Information Network (SCINET)

- Defense Information Systems Network (DISN)

- Integrated Tactical Strategic Data Network (ITSDN)

- Critical Intelligence Communications (CRITICOMM) System

- Special Intelligence Communication (SPINTCOM) Network

- STU-III (Secure Telephone Unit-III)

- Red Switch

Table B-1. Identification of Service DAAs and Applicable Policies

Type of Information Processed	Applicable Policy(ies)	Navy DAA	Marine Corps DAA	Army DAA	Air Force DAA
Special Intelligence (All classification levels)	NSA/CSS 10•27 NSA/CSS 90-5	NSA/Central Security Service (CSS)	NSA/CSS	NSA/CSS	NSA/CSS
Sensitive Compartmented Information (SCI) (All classification levels)	DCID 1/16 DCID 1/19 DIAM 50-3 DIAM 50-4	DIA/DS-SIM DNI	DIA/DS-SIM Director, Intelligence Div. (CMC Code INT)	DIA/DS-SIM MACOM Commander, Heads of DA Staff Agencies (dedicated mode); HQDA (DAMI-CIC-AS) (Other Modes)	DIA/DS-SIM HQ USAF/INS, AFIS/IND
SIOP-ESI (All classification levels)	MJCS 75-87	JCS/J36; coordinate with Chief of Naval Operations (CNO)	JCS/J36; coordinate with CNO	JCS/J36; coordinate with HQDA (DAMI-CIC-AS)	JCS/J36; coordinate with HQ USAF/XOX
Top Secret (All classification levels)	DoD Policies*, Appropriate Service Policies**	Commander	CMC (Code CC)	MACOM Commander, Heads of DA Staff Agencies	MAJCOM Commander
Secret/Confidential (All classification levels)	DoD Policies*, Appropriate Service Policies**	Commander	Commanding General	MACOM Commander, Heads of DA Staff Agencies, General Officer Commanders	MAJCOM Commander
Sensitive Unclassified	DoD Policies*, Appropriate Service Policies**	Commander	Director of AIS Activity	Post, installation, or field operation or staff support activity commanders or equivalent	MAJCOM Commander

* DoD policies include DoDD 5200.28, 5200.28-STD, 5200.28-M, and other DoD policies for each security discipline, as listed in section 4.1.2.

** Appropriate service/agency policies include the primary service/agency policy as listed in Appendix C and other service/agency or command-level policies, as appropriate, in the other security disciplines.

49

Table B-2. Identification of Other Agency DAAs

Type of Information Processed	Applicable Policy(ies)	DIA DAA	NSA DAA	DISA DAA	JCS DAA	DLA DAA	DMA DAA	DNA DAA	Other Agency DAA
Special Intelligence (All classification levels)	NSA/CSS 10-27 NSA/CSS 90-5	NSA/ Central Security Service (CSS)	NSA/CSS	NSA/ CSS	NSA/ CSS	NSA/CSS	NSA/CSS	NSA/CSS	NSA/CSS
Sensitive Compartmented Information (SCI)(All classification levels)	DCID 1/16 DCID 1/19 DIAM 50-3 DIAM 50-4	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM	DIA/ DS-SIM
SIOP-ESI (All classification levels)	MJCS 75-87	JCS/J36; coordinate with DS-SIM	JCS/J36; coordinate with J06	JCS/J36	JCS/J36	JCS/J36; coordinate with DLA-I	JCS/J36; coordinate with HQ-IS	JCS/J36	JCS/J36
Top Secret (All classification levels)	DoD Policies*, Appropriate Agency Policies**	DIA/ DS-SIM	NSA/Office of Operational Computer Security	Director, DISA	Director Joint Staff or Director J6	Deputy Director/ PLFA Commander		HQDNA	
Secret/ Confidential (All classification levels)	DoD Policies*, Appropriate Agency Policies**	DIA/ DS-SIM	NSA/Office of Operational Computer Security	Director, DISA	Director Joint Staff or Director J6	Deputy Director/ PLFA Commander		Appropriate DAA	
Sensitive Unclassified	DoD Policies*, Appropriate Agency Policies**	DIA/ DS-SIM	NSA/Office of Operational Computer Security	Director, DISA	Director Joint Staff or Director J6	Deputy Director/ PLFA Commander		Appropriate DAA	

*   DoD policies include DoDD 5200.28, 5200.28-STD, 5200.28-M, and other DoD policies for each security discipline, as listed in section 4.1.2.

**   Appropriate service/agency policies include the primary service/agency policy as listed in Appendix C and other service/agency or command-level policies, as appropriate, in the other security disciplines.

Table B-3. DAAs for Separately Accredited Networks

Network	Applicable Policies	Security Mode of Operation	DAA(s)***
AUTODIN/ DMS	DCAC 370-195-3	Multilevel	DISA/DA DIA/DS-SIM JCS/(DJS/J6) NSA/Office of Operational Security
DSN		System High	DISA
MILNET	DoD Policies*	System High	DISA/DA
DSNET1	DoD Policies*	System High	DISA/DA
DSNET2	DoD Policies*	System High	JCS/J6
DSNET3	DCID 1/16**	System High	DIA/DS-SIM
DISN		System High	DISA
ITSDN		Multiple System High Nets	DISA/DIA/NSA/JCS
CRITICOMM	NSA Policies	System High	NSA/Office of Operational Security
SPINTCOM	DCID 1/16**	System High	DIA/DS-SIM
STU III		Multilevel	NSA
Red Switch	DCID 1/16** DoDD C-5030.58	System High	DIA

*   DoD policies include DoDD 5200.28, 5200.28-STD, 5200.28-M, and other DoD policies for each security discipline, as listed in section 4.1.2.

**   Includes DCI policies for the other security disciplines as well.

*** For some networks, the DAA(s) depends on the accreditation range of the network. The applicable policy(ies) should be consulted for additional information in this area.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX   C

DOD COMPONENT AIS SECURITY POLICIES

The following list identifies selected DoD references in some INFOSEC security disciplines. Each service/agency has its own security regulations that implement DoDD 5200.28 and the other DoD policies for each security discipline. The primary service/agency security policies are the following:

- DoD, 7 June 1982, *Information Security Program*, DoDD 5200.1, and June 1986, with Change No.1, 27 June 1988, *Information Security Program Regulation,* DoD 5200.1-R [19].

- DoD, October 1981, *Communications Security (COMSEC)* (U), DoDD C-5200.5, (This document is classified.) 20].

- DoD, February 1990, *Control of Compromising Emanations* (U), DoDD C-5200.19, (This document is classified.) [5].

- NSA/Central Security Service (CSS), December 1990, *TEMPEST Security Program*, NSA/CSS Regulation 90-5 [21].

- NTISSC, October 1988, *TEMPEST Countermeasures for Facilities* (U), NTISS Instruction (NTISSI) 7000, (This document is classified.) [22].

- DoD, July 1980, *Security of Military Installations and Resources*, DoDD 5200.8 [23].

- DoD, April 1984, *Security of DoD Communications Facilities*, DoDD 5210.73 [24].

- DIA, *Physical Security Standards for Construction of Sensitive Compartmented Information Facilities* (U), DIA Manual (DIAM) 50-3, (For Official Use Only (FOUO)) [25].

- DCI, September 1987, *U.S. Intelligence Community Physical Standards for Sensitive Compartmented Information*, DCID 1/12 [26].

- DoD, December 1979, *DoD Personnel Security Program*, DoDD 5200.2 [27].

- DCI, April 1986, *Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, DCID 1/14 [28].

- DoD, July 1983, *DoD Operations Security Program*, DoDD 5205.2 [29].

- DoD, September 1986, *Computer Security Technical Vulnerability Reporting Program*, DoD Instruction 5215.2 [30].

- DoD, July 1978, *Defense Special Security Communications System: Security Criteria and Telecommunications Guidance*, DoD C-5030.58-M [31].

- Defense Communications Agency (DCA), March 1987, *DCS AUTODIN Category III Operational Acceptance Test*, DCA Circular (DCAC) 370-D195-3 [32].

- DoD, December 1985, *Industrial Security Regulation*, DoDD 5220.22-R [33], and January 1991, *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M [34] (issued under the authority of DoDD 5220.22, *DoD Industrial Security Program*, December 1980).

- Department of the Air Force, 2 June 1992, *The Air Force Computer Security (COMPUSEC) Program*, Air Force System Security Instruction (AFSSI) 5100.[35]

- Department of the Air Force, May 1983, *Control of Dissemination of Intelligence Information*, AFR 205-19 [36].

- Department of the Navy, November 1989, *Department of the Navy Automated Information Systems (AIS) Security Program*, Secretary of the Navy Instruction (SECNAVINST) 5239.2 [37] (under revision as of date of this document).

- Department of the Navy, April 1985, *Department of the Navy Automated Data Processing Security Program*, Office of the Chief of Naval Operations Instruction (OPNAVINST) 5239.1A [38].

- Department of the Navy, July 1990, *Department of the Navy SCI/Intelligence, Automated Information Systems (AIS) Security Program*, Naval Intelligence Command Instruction (NAVINTCOMINST) 5239.3 [39].

- Marine Corps, 1982, *Marine Corps Automatic Data Processing Security Manual*, Marine Corps Order (MCO) Publication 5510.14, Change 1 [40].

- Department of the Army, August 1990, *Information Systems Security*, AR 380-19 [7].

- Defense Intelligence Agency (DIA), 1980, *Security of Compartmented Computer Operations* (U), DIA Manual (DIAM) 50-4, (This document is classified.) [41].

- DIA, March 1979, *Security Requirements for Automatic Data Processing (ADP) Systems*, DIA Regulation 50-23 [42].

- NSA, January 1990, *Security for Automated Information Systems and Networks* (U), NSA/Central Security Service (NSA/CSS) Directive No. 10-27, (FOUO) [43].

- NSA, 17 October 1990, *NSA/CSS Operational Computer Security Manual*, NSA/CSS Manual 130-1 [44].

- Joint Chiefs of Staff (JCS), April 1988, *Security Policy for the WWMCCS Intercomputer Network*, JCS Pub 6-03.7 (applies to all Worldwide Military Command and Control Systems (WWMCCS) sites) [45].

- JCS, May 87, *Safeguarding the Single Integrated Operational Plan (U)*, *Memorandum*, JCS (MJCS) 75-87 (applies to all systems processing SIOP-ESI), (This document is classified.) [46] (under revision as of date of this document).

- DCI, February 1987, *Security Policy for Sensitive Compartmented Information*, DCID 1/19 [47].

- Defense Information Systems Agency (DISA), August 1991, *Security Requirements for Automated Information Systems (AISs)*, DCA Instruction 630-230-19 [48].

- Defense Mapping Agency (DMA), July 1990, *Automated Information Systems Security Requirements*, DMA Manual 5200.28 [49] (under revision as of date of this document).

- *Defense Nuclear Agency (DNA), 31 August 1989, Security Requirements for Automated Information Systems (AISs)*, DNA 5200.28D [50] (under revision as of date of this document).

- Defense Logistics Agency (DLA), October 1991, *Security Requirements for Automated Information and Telecommunications Systems*, DLA Regulation (DLAR) 5200.17 [51].

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

ACRONYMS

ADP	Automatic Data Processing
AF	Air Force
AFR	Air Force Regulation
AFSSI	Air Force System Security Instruction
AIS	automated information system
AR	Army Regulation
AUTODIN	Automatic Digital Network
C&A	certification and accreditation
CAP	component approval process
CMC	Commandant, Marine Corps
CMW	compartmented mode workstation
CMWEC	CMW Evaluation Criteria
CNO	Chief of Naval Operations
COMPUSEC	computer security
COMSEC	communications security
CONOPS	concept of operation
COTS	commercial off-the-shelf
CRITICOMM	Critical Intelligence Communications
CSS	Central Security Service (of NSA)
DA	Department of the Army
DAA	Designated Approving Authority
DBMS	database management system
DCA	Defense Communications Agency (now DISA)
DCAC	DCA Circular
DCI	Director of Central Intelligence
DCID	DCI Directive
DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DIAM	DIA Manual
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLA	Defense Logistics Agency
DLAR	DLA Regulation
DMA	Defense Mapping Agency
DMS	Defense Message System
DNA	Defense Nuclear Agency

DNI	Director of Naval Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DPL	Degausser Products List
DSNET1	Defense Secure Network 1
DSNET2	Defense Secure Network 2
DSNET3	Defense Secure Network 3
EO	Executive Order
EPL	Evaluated Products List
ETL	Endorsed Tools List
FIPS PUB	Federal Information Processing Standard Publication
FOUO	For Official Use Only
FSRS	Functional Security Requirements for a Telecommunications System
HQDA	Headquarters, Department of the Army
HQDNA	Headquarters, Defense Nuclear Agency
IC	Intelligence Community
INFOSEC	information systems security
ISSWG	Information System Security Working Group
ITSDN	Integrated Tactical Strategic Data Network
IV&V	independent verification and validation
JCS	Joint Chiefs of Staff
LAN	local area network
MACOM	Major Command (Army)
MAJCOM	Major Command (Air Force)
MCO	Marine Corps Order
MILNET	Military Network
MJCS	Memorandum, JCS
MLS	multilevel secure
MOA	Memorandum of Agreement
NAVINTCOMINST	Naval Intelligence Command Instruction
NCSC	National Computer Security Center or National Communications Security Committee
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSD	National Security Directive
NSTISS	National Security Telecommunications and Information Systems Security
NTISS	National Telecommunications and Informations Systems Security

NTISSI	National Telecommunications and Informations Systems Security Instruction
OMB	Office of Management and Budget
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPSEC	operations security
OSD	Office of the Secretary of Defense
PC	personal computer
PLFA	Primary-Level Field Activity
PM	Program Manager
PPL	Preferred Products List
RFP	Request for Proposal
SCI	Sensitive Compartmented Information
SCINET	Sensitive Compartmented Information Network
SECNAVINST	Secretary of the Navy Instruction
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information
SPINTCOM	Special Intelligence Communication
STU-III	Secure Telephone Unit-III
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TECHSEC	technical security
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
TNI	Trusted Network Interpretation
TRANSEC	transmission security
TSCM	technical surveillance countermeasures
U	Unclassified
U.S.	United States
USA	United States Army
USAF	United States Air Force
USN	United States Navy
WAN	wide area network
WINCS	WWMCCS Information Network Computer System
WWMCCS	Worldwide Military Command and Control System

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

List of References

1. Department of Defense (DoD), 21 March 1988, *Security Requirements for Automated Information Systems (AISs)*, DoD Directive 5200.28.

2. DoD, December 1985, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD.

3. Defense Intelligence Agency (DIA), June 1991, *Compartmented Mode Workstation Evaluation Criteria, Version 1 (CMWEC)*, document number DDS-2600-6243-91.

4. NSA, 2 June 1991, *NSA Specification for General Functional Security Requirements for a Telecommunications System,* (FSRS)(U). (This document is classified.)

5. DoD, February 1990, *Control of Compromising Emanations (U)*, DoDD C-5200.19, (This document is classified.)

6. DCI, 19 July 1988, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, DCID 1/16, (This document is classified.), and *Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)*, supplement to DCID 1/16, (This document is classified).

7. Department of the Army, August 1990, *Information Systems Security*, AR 380-19.

8. Office of the President, July 1990, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, (This document is classified.).

9. Executive Order 12356, 2 April 1982, *National Security Information.*

10 Executive Order 12333, 4 December 1981, *United States Intelligence Activities.*

11. Office of Management and Budget (OMB), 12 December 1985, *Management of Federal Information Resources*, OMB Circular No. A-130. (Revision currently in process.).

12. National Institute of Standards and Technology (NIST), 27 September 1983, *Guideline for Computer Security Certification and Accreditation*, FIPS PUB 102.

13. Public Law 100-235, 101 STAT. 1724, 8 January 1988, *Computer Security Act of 1987.*

14. National Computer Security Center, 31 July 1987, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria,* NCSC-TG-005, Version-1.

15. DoD, January 1973, *Automated Information System Security Manual,* DoD 5200.28-M. (Revision currently in process.).

16. NSA, *Information Systems Security Products and Services Catalogue (INFOSEC Catalog).*

17. NIST, April 1982, *General Security Requirements for Equipment Using the Data Encryption Standard,* Federal Standard 1027.

18. Title 5, U.S. Code, Section 552a, *Privacy Act of 1974.*

19. DoD, 7 June 1982, *Information Security Program,* DoD Directive 5200.1, and June 1986, with Change No. 1, 27 June 1988, *Information Security Program Regulation,* DoD 5200.1-R.

20. DoD, October 1981, *Communications Security (COMSEC) (U),* DoDD C-5200.5, (This document is classifed.).

21. NSA/CSS, December 1990, *TEMPEST Security Program,* NSA/CSS Regulation 90-5.

22. NTISSC, October 1988, *TEMPEST Countermeasures for Facilities (U),* NTISSI 7000, (This document is classified.).

23. DoD, July 1980, *Security of Military Installations and Resources,* DoDD 5200.8.

24. DoD, April 1984, *Security of DoD Communications Facilities,* DoDD 5210.73.

25. DIA, *Physical Security Standards for Construction of Sensitive Compartmented Information Facilities (U),* DIAM 50-3, (This document is for offical use only.).

26. DCI, September 1987, *U.S. Intelligence Community Physical Standards for Sensitive Compartmented Information,* DCID 1/12.

27. DoD, December 1979, *DoD Personnel Security Program,* DoDD 5200.2.

28. DCI, April 1986, *Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information,* DCID 1/14.

29. DoD, July 1983, *DoD Operations Security Program,* DoDD 5205.2.

30. DoD, September 1986, *Computer Security Technical Vulnerability Reporting Program*, DoD Instruction 5215.2.

31. DoD, July 1978, *Defense Special Security Communications System: Security Criteria and Telecommunications Guidance*, DoD C-5030.58-M.

32. DCA, March 1987, *DCS AUTODIN Category III Operational Acceptance Test*, DCAC 370-D195-3.

33. DoD, December 1985, *Industrial Security Regulation*, DoD Regulation 5220.22-R.

34. DoD, January 1991, *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M.

35. Department of the Air Force, 2 June 1992, *The Air Force Computer Security (COMPUSEC) Program*, AFSSI 5100.

36. Department of the Air Force, May 1983, *Control of Dissemination of Intelligence Information*, AFR 205-19.

37. Department of the Navy, November 1989, *Department of the Navy Automated Information Systems (AIS) Security Program*, SECNAVINST 5239.2.

38. Department of the Navy, April 1985, *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1A.

39. Department of the Navy, July 1990, *Department of the Navy SCI/Intelligence, Automated Information System (AIS) Security Program*, NAVINTCOMINST 5239.3.

40. Marine Corps, 1982, *Marine Corps Automatic Data Processing Security Manual*, MCO P5510.14, Change 1.

41. DIA, 1980, *Security of Compartmented Computer Operations (U)*, DIAM 50-4, (This document is classified.).

42. DIA, March 1979, *Security Requirements for Automatic Data Processing (ADP) Systems*, DIA Regulation 50-23.

43. NSA, January 1990, *Security for Automated Information Systems and Networks (U)*, NSA/CSS Directive No. 10-27, (This document is for official use only.).

44. NSA, 17 October 1990, *NSA/CSS Operational Computer Security Manual*, NSA/CSS Manual 130-1.

45. JCS, April 1988, *Security Policy for the WWMCCS Intercomputer Network*, JCS Pub 6-03.7.

46. JCS, May 1987, *Safeguarding the Single Integrated Operational Plan (U)*, MJCS 75-87, (This document is classified) (under revision as of date of this document).

47. DCI, February 1987, *Security Policy for Sensitive Compartmented Information*, DCID 1/19.

48. Defense Information Systems Agency (DISA), August 1991, Security *Requirements for Automated Information Systems (AISs)*, DCA Instruction 630-230-19.

49. Defense Mapping Agency (DMA), July 1990, *Automated Information Systems Security Requirements*, DMA Manual 5200.28 (under revision as of date of this document).

50. Defense Nuclear Agency (DNA), 31 August 1989, *Security Requirements for Automated Information Systems (AISs)*, DNA 5200.28D (under revision as of date of this document).

51. Defense Logistics Agency (DLA), October 1991, *Security Requirements for Automated Information and Telecommunications Systems*, DLA Regulation (DLAR) 5200.17.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE January 1994	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE
Introduction to Certification and Accreditation

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Security Agency
Attention: Standards, Criteria, and Guidelines Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
NCSC-TG-029
Version 1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Security Agency
9800 Savage Rd.
Ft. Meade MD 20755-6000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
Library No., S-239,954

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release: Unlimited Distribution

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This document, which provides an introduction to certification and accreditation (C&A), provides an introductory discussion of some basic concepts related to C&A and sets the baseline for further documents. Its objectives are the following: (1) to provide an overview of C&A; (2) to clarify the critical roles the Designated Approving Authority (DAA) and other key security officials must assume throughout the C&A process; (3) to identify some key policy issue areas; and (4) to define C&A-related terms. The details of the actual C&A process are not included in this document, but will be provided in follow-on documents.

14. SUBJECT TERMS
Certification, Accreditation, Designated Approving Authority (DAA), INFOSEC, Security policy, Computer Security

15. NUMBER OF PAGES
76

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19 SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT